Network Fault Tolerance Analysis

Redstone Delivery

Checkout and Launch Control Systems (CLCS)

84K00232

Approved By:

Preparer Date

Lead – CLCS Networks Date

Date

Date

Date

Date

PREPARED BY: Steven Goodmark

REVISION HISTORY

REV	DESCRIPTION	DATE
Basic	Promoted per approval by signatories. Updated and changed document title to standard format. ljp	5/11/98

LIST OF EFFECTIVE PAGES

Dates of issue of change pages are:

Page No.	**A or D***	**Issue or Change No.**	**CR No.**	**Effective Date****

Table of Contents

List of Figures

NETWORK FAULT TOLERANCE ANALYSIS

1. INTRODUCTION

1.1 IDENTIFICATION

This is the Redstone Delivery Network Fault Tolerance Analysis for the Checkout and Launch Control System (CLCS), Document 84K00232 Rev. BASIC. This document addresses the fault tolerance of the Display and Control Network (DCN) Hardware Configuration Item (HWCI) and the Real Time Critical Network (RTCN) HWCI.

1.2 PURPOSE

The purpose of this document is to assess the RTCN and DCN fault tolerance of the CLCS Real Time Processing System (RTPS). This analysis is performed with respect to the baseline architecture, requirements and project Statement of Work (SOW) for the Redstone delivery.

1.3 CSCI / HWCI OVERVIEW

The Network Services CSC / HWC of the System Services CSCI / HWCI provides the inter-platform data transport for the CLCS. Inter-platform data transport occurs between VME/VxWorks Gateway platforms, Silicon Graphics Origin 2000 based Data Display Processors (DDPs), Command and Control Processors (DDPs), and the Shuttle Data Center (SDC) over the RTCN. Inter-platform data transport occurs between Origin 2000 based Data Display Processors, Command Control Processors, Silicon Graphics O2 based Human Computer Interface (HCI) platforms, and the SDC over the DCN. The communication protocol used for mission critical data transfer is Reliable Messaging (RM) developed by the CLCS Network Services CSC System Services CSCI. This protocol handles any required retransmissions of data.

1.4 ASSUMPTIONS

1. Fault tolerance analysis is based on single event failures.
2. The DCN is baselined as ring based FDDI.
3. End item redundancy is not included (backup gateways, DDP, CCP, etc.).
4. The RTCN is baselined as switched 100BaseT.
5. The Utility Networks are not included.
6. Power source is considered a single point of failure.

1.5 CUSTOM AND COTS SOFTWARE

The fault tolerance analysis reveals a distinction in the operation of custom and commercial-off-the-shelf (COTS) software. Figure 1-1, below, illustrates the operation of custom and COTS software with respect to the network protocol stack. Custom software utilizes the RM protocol while COTS software interfaces directly with the Transmission

Control Protocol (TCP) and User Datagram Protocol (UDP) application programming interfaces (APIs). Custom software interface fail over capability is provided by the RM protocol. This leaves the COTS software with only standard TCP and UDP APIs. The result is COTS software is not provided with any capability for interface fail over.

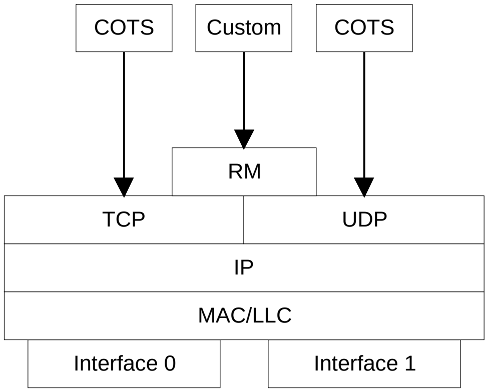

Figure 1-1, RM Protocol Stack

1.6 DOCUMENT ORGANIZATION

This document is divided into three sections and four appendices:

Section 1, Scope, discusses the purpose of the CSCI/HWCI analysis, provides a system overview , and describes software and hardware configurations for the system.

Section 2, Applicable Documents, lists the documents used to create and those supporting this document.

Section 2, RTCN Failure Scenarios, contains the description and analysis of RTCN test cases.

Section 3, DCN Failure Scenarios, contains the description and analysis of DCN test cases.

Section 4, Conclusion, contains conclusions compiled from all test cases.

Appendix A, Acronyms and Definitions, contains a listing of acronyms and selected word definitions (for words which may have multiple interpretations)

Appendix B, Requirements Traceability and Test Methods Matrix, contains the requirements verification matrix for the test.

2. APPLICABLE DOCUMENTATION

The following documents, of the revision shown, form a part of this document to the extent specified.

2.1 PARENT DOCUMENTS

The documents in this paragraph establish the criteria and technical basis for the existence of this document. The parent documents are:

Parent Document	Document Number	Rev.	Date
N/A			

Table 2.1: Parent Documents

2.2 APPLICABLE DOCUMENTS

Applicable documents are those documents which form a part of this document. These documents, at the revisions listed below, carry the same weight as if they were stated within the body of this document.

Applicable Document	Document Number	Rev.	Date
N/A			

Table 2.2: Applicable Documents

2.3 REFERENCE DOCUMENTS

Reference documents are those documents which, though not a part of this document, serve to clarify the intent and contents of this document.

Reference Document	Document Number	Rev.	Date
N/A			

Table 2.3: Reference Documents

3. RTCN FAILURE SCENARIOS

3.1 NOMINAL OPERATION FOR ACTIVE/STANDBY OPERATION

3.1.1 Description

Figure 3-1 indicates active data paths in the RTCN under nominal conditions. Interface 0 / Switch Group 0 is designated the default primary path.

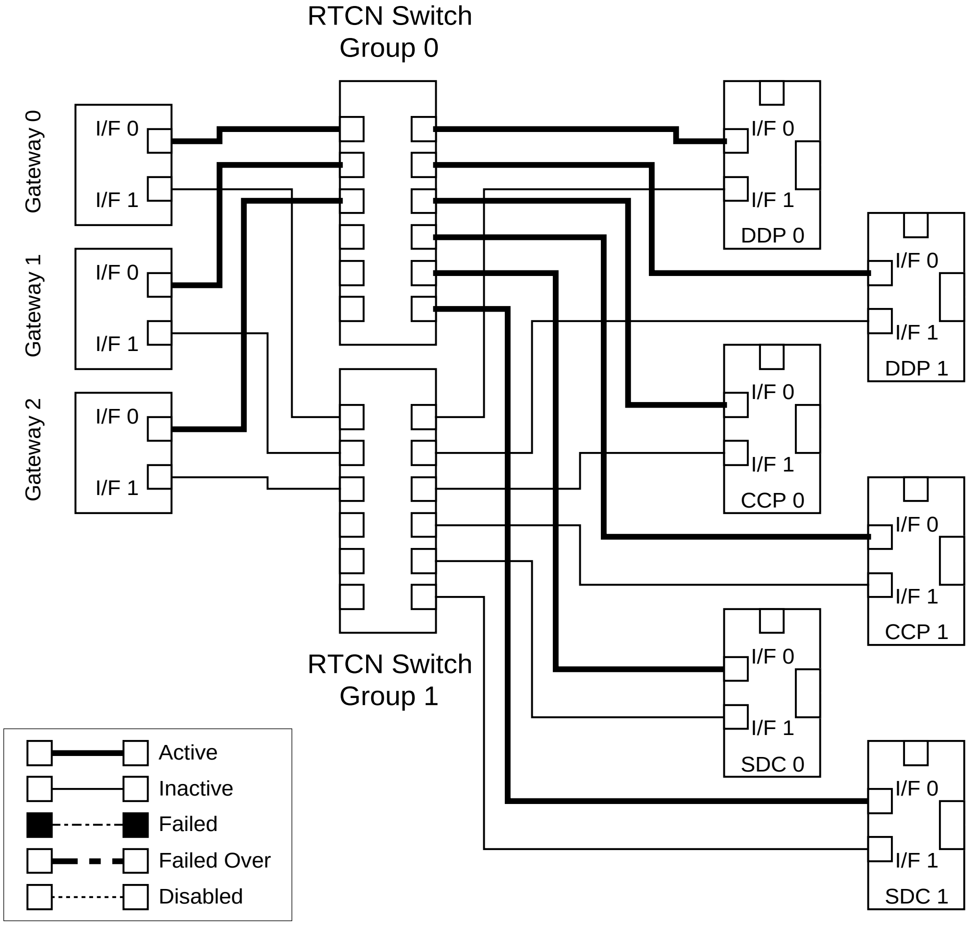

Figure 3-1, RTCN Nominal Operation

For the purpose of this analysis, the communication flows have been identified as:

1. Data transmission:
   a) Change Data flows from the Gateway to the DDP and SDC with associated acknowledgments.
   b) Data Distribution Data flows from the DDP to the CCP and SDC with associated acknowledgments.
2. Commanding:

a) Commands flow from the CCP to the Gateway and SDC with associated acknowledgments.

b) Command Responses flow from the Gateway to the CCP and SDC with associated acknowledgments.

3.2 FAILURES FOR ACTIVE/STANDBY OPERATION

The following sections detail the single point failures identified for the RTCN

3.2.1 Gateway NIC Failure, Single Fail Over

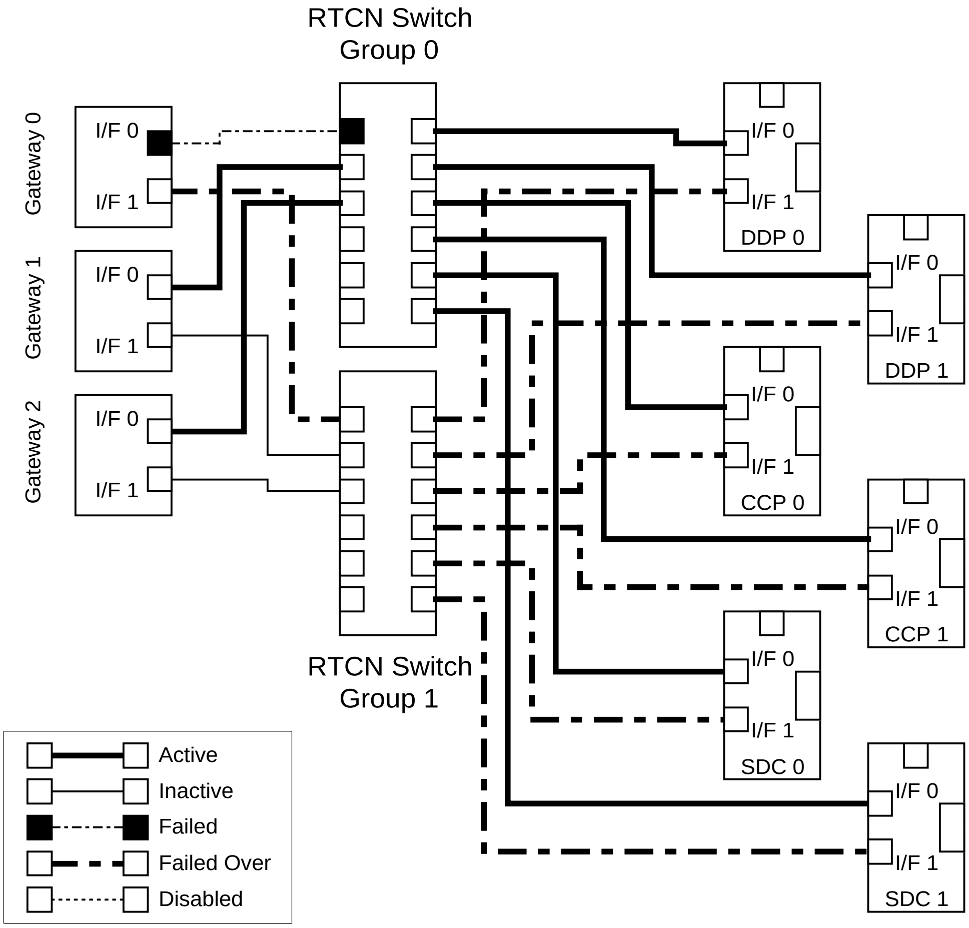

Figure 3-2, Gateway NIC Failure, Single Device Fails Over

Figure 3-2 illustrates the case where Gateway 0 interface 0 to the RTCN fails and begins ingesting commands and transmitting change data and command responses on its interface 1. Only the failed link fails over. All devices communicating with Gateway 0 over interface 0 must now communicate over interface 1. This results in the RTCN having two active networks. (The data flow over RTCN Switch Group 1 requires all DDP, CCP, and SDC interfaces on Group 1 be active and monitored in parallel with those on Group 0.)

3.2.2 Gateway NIC Failure, All Fail Over

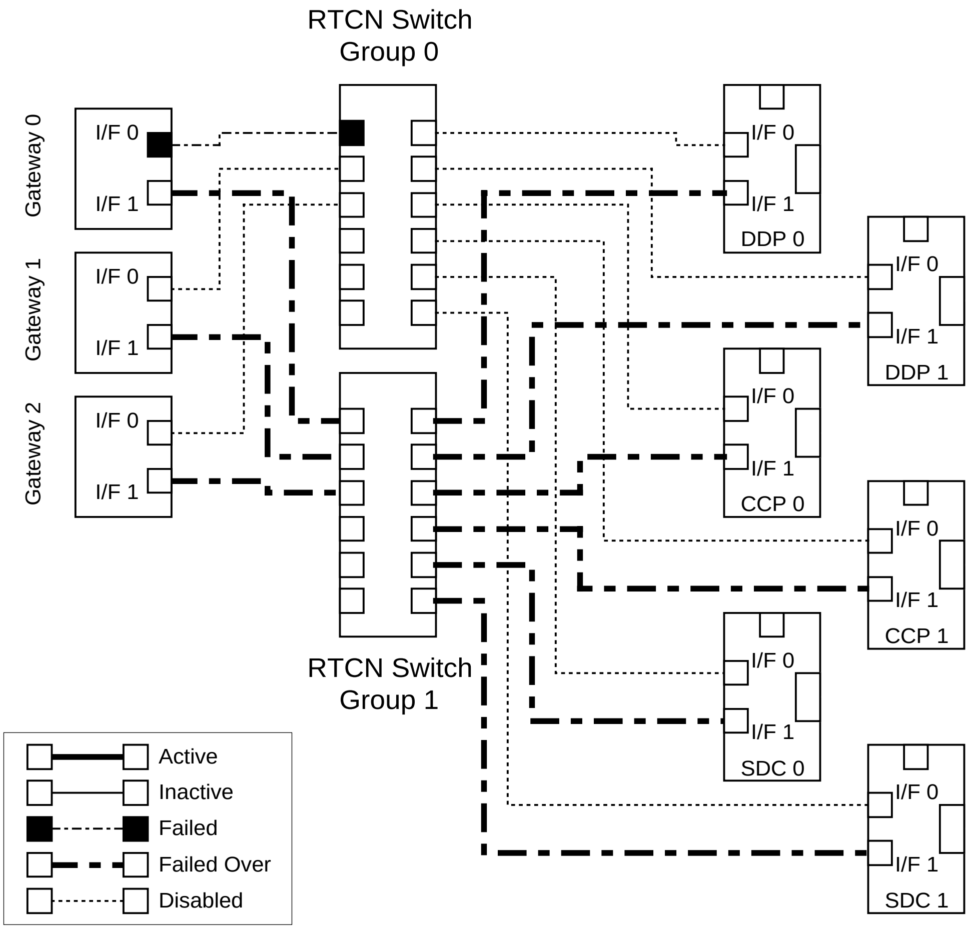

Figure 3-3, Gateway NIC Failure, All Devices Fail Over

Figure 3-3 illustrates the case where Gateway 0 interface 0 to the RTCN fails and begins ingesting commands and transmitting change data and command responses on its interface 1. This scenario assumes that the system software swings all data flows onto the secondary paths and completely idles the primary path.

3.2.3 DDP NIC Failure, Single Fail Over

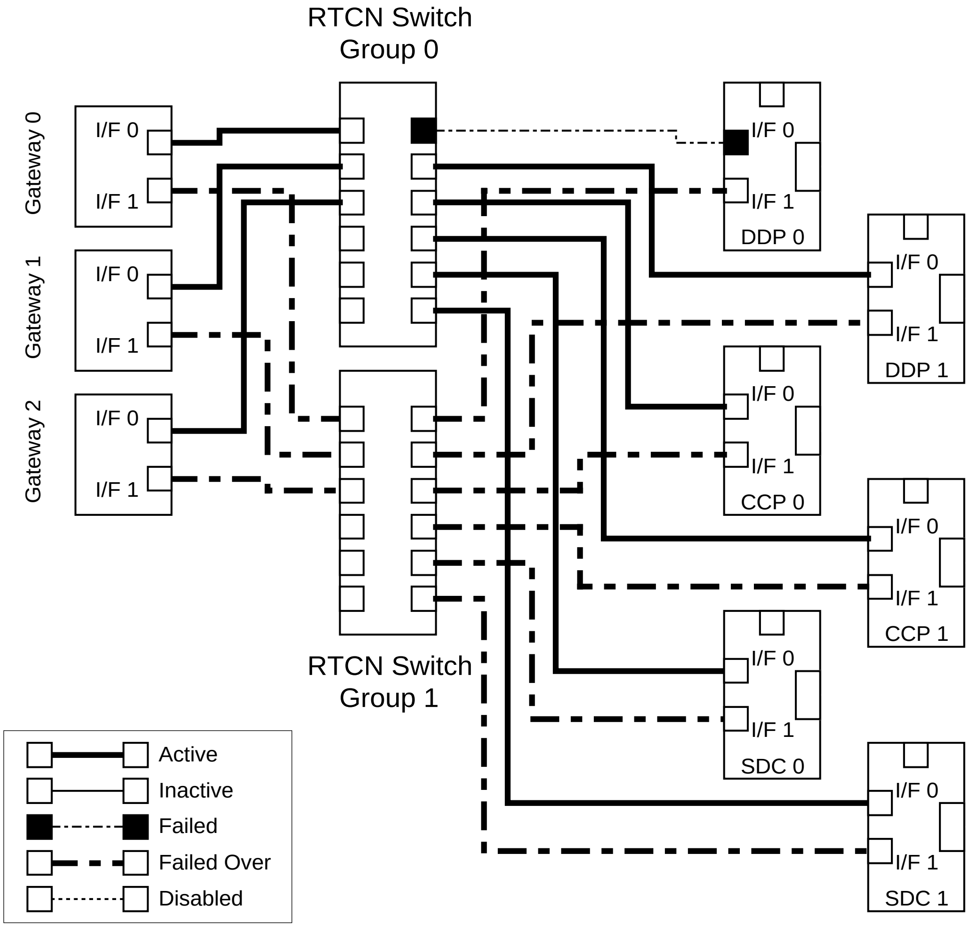

Figure 3-4, DDP NIC Failure, Single Device Fails Over

Figure 3-4 illustrates the case where DDP 0 interface 0 to the RTCN fails. The DDP begins ingesting change data and originating data distribution data on its interface 1. Only the failed link fails over. All devices communicating with DDP 0 over interface 0 must now communicate over interface 1. This results in the RTCN having two active networks. (The data flow over RTCN Switch Group 1 requires all DDP, CCP, Gateway, and SDC interfaces on Group 1 be active in parallel with those on Group 0.)

3.2.4 DDP NIC Failure, All Fail Over

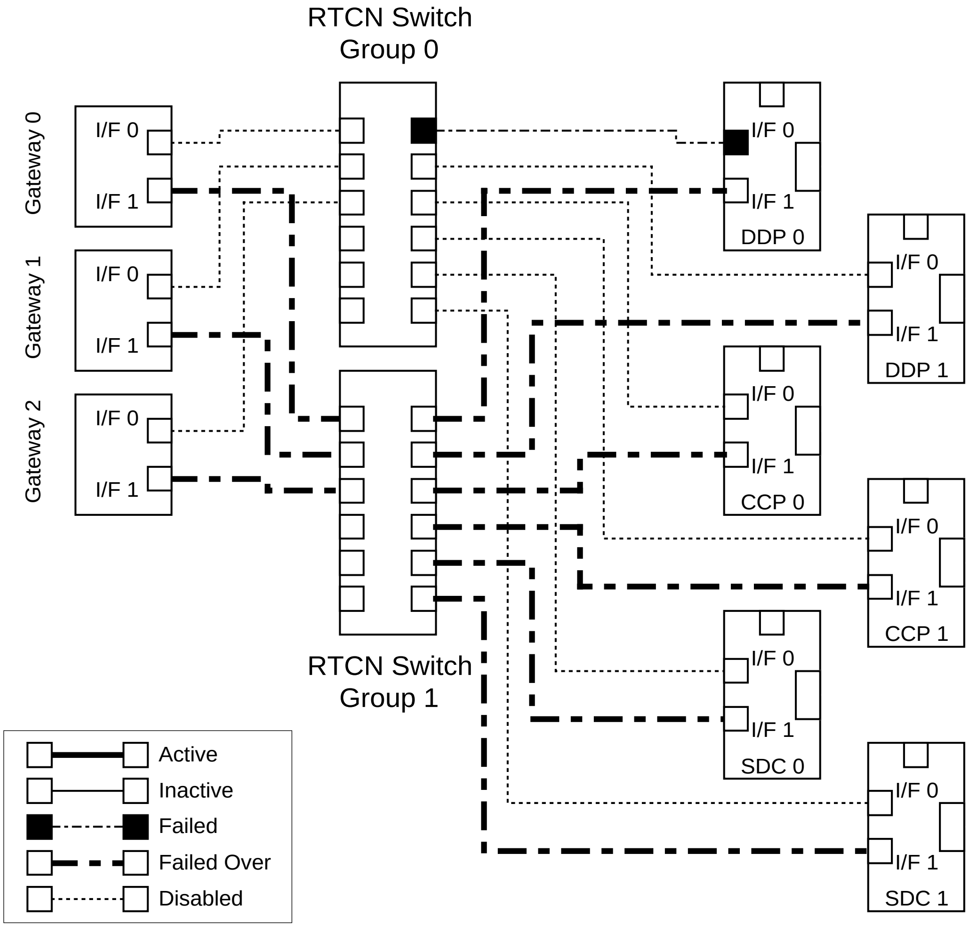

Figure 3-5, DDP NIC Failure, All Devices Fail Over

Figure 3-5 illustrates the case where DDP 0 interface 0 to the RTCN fails. The DDP begins ingesting change data and originating data distribution data on its interface 1. This scenario assumes that the system software swings all data flows onto the secondary paths and completely idles the primary path.

3.2.5 CCP NIC Failure, Single Fail Over

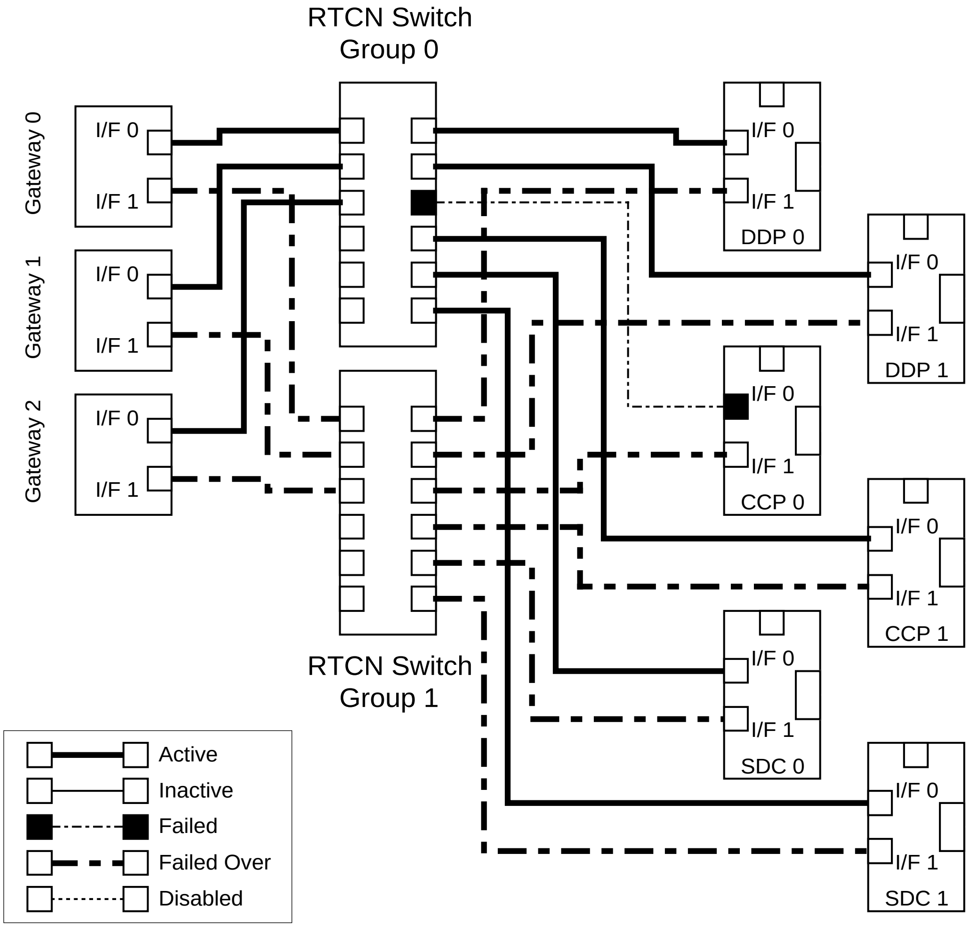

Figure 3-6, CCP NIC Failure, Single Device Fail Over

Figure 3-6 illustrates the case where CCP 0 interface 0 to the RTCN fails. The CCP begins ingesting data distribution data and command responses and originating commands on its interface 1. Only the failed link fails over. All devices communicating with Gateway 0 over interface 0 must now communicate over interface 1. This results in the RTCN having two active networks. (The data flows over RTCN Switch Group 1 requires all DDP, CCP, Gateway, and SDC interfaces on Group 1 be active in parallel with those on Group 0.)

3.2.6 CCP NIC Failure, All Fail Over

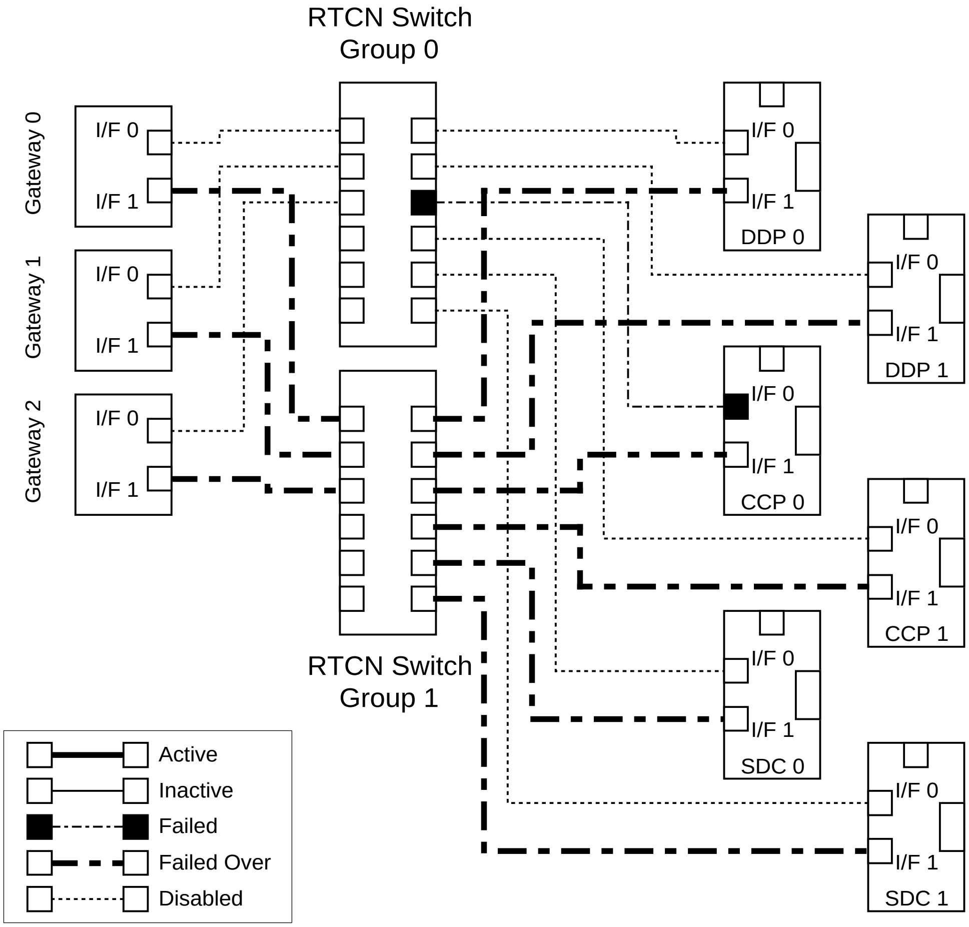

Figure 3-7, CCP NIC Failure, All Devices Fail Over

Figure 3-7illustrates the case where CCP 0 interface 0 to the RTCN fails. The CCP begins ingesting data distribution data and command responses and originating commands on its interface 1. This scenario assumes that the system software swings all data flows onto the secondary paths and completely idles the primary path.

3.2.7 SDC Failure, Record Only

Failure of an SDC port is a special case. The SDC is chartered to record all data and acknowledgments. Therefore a failure in any single port would require a complete SDC MUX fail over. The question then becomes why should SDC port failure drive a fail over in the Gateway, DDP, and CCP paths? Operations are not directly impacted by loss of an SDC port.

3.2.7.1 SDC NIC Failure, No Fail Over

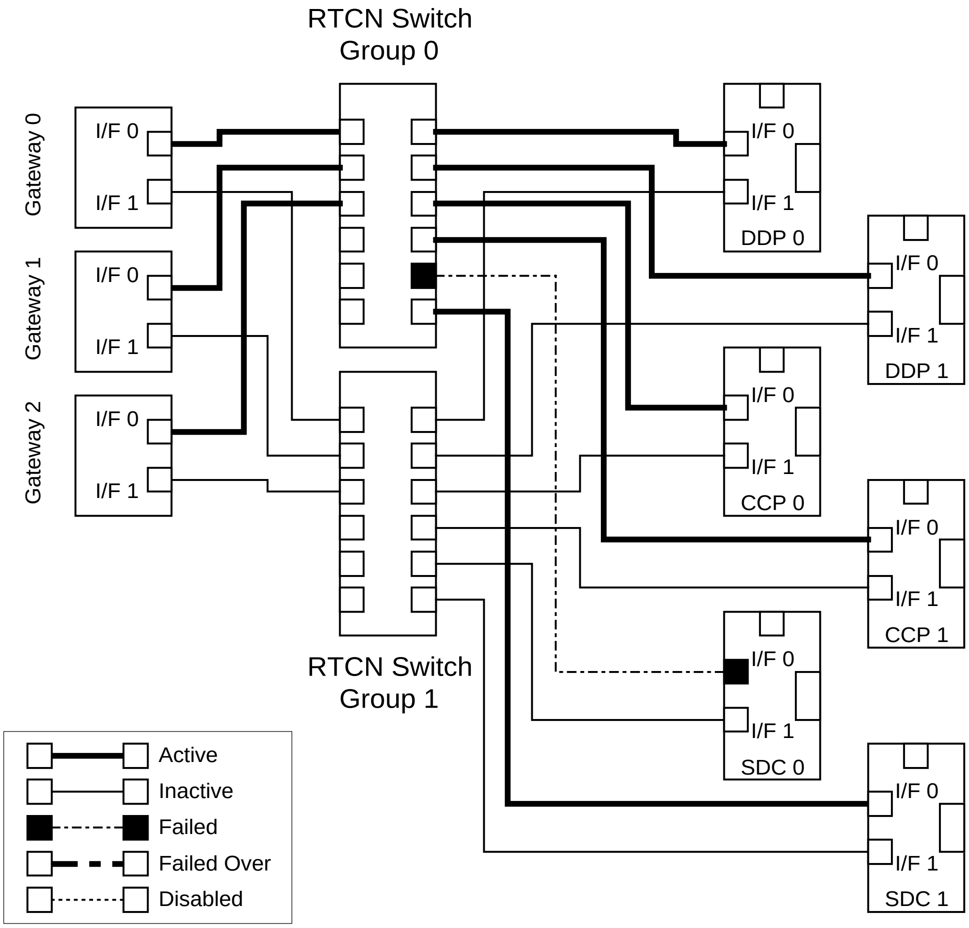

Figure 3-8, SDC NIC Failure, No Fail Over

Figure 3-8 illustrates the case where SDC 0 interface 0 to the RTCN fails. System Integrity directs SDC ingestion through the secondary SDC MUX without initiating any RM fail over.

3.2.7.2 SDC NIC Failure, Single Fail Over

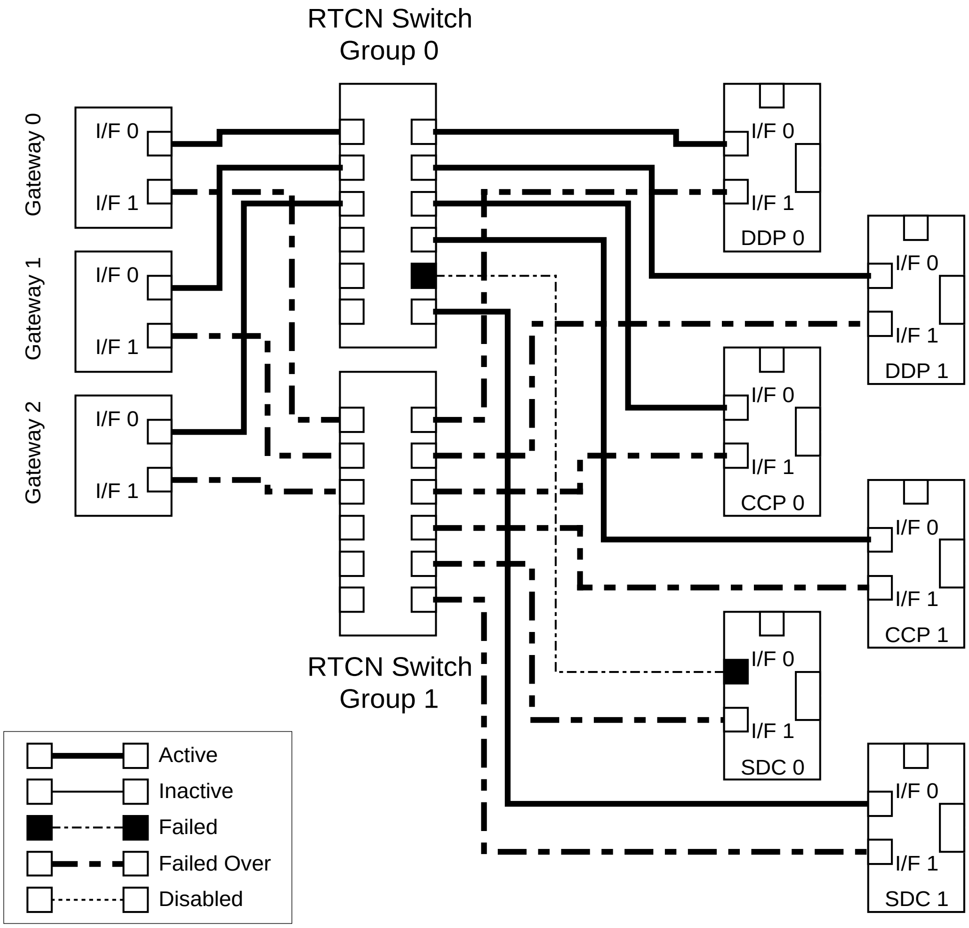

Figure 3-9, SDC NIC Failure, Single Device Fail Over

Figure 3-9 illustrates the case where SDC 0 interface 0 to the RTCN fails. The SDC begins ingesting data on its interface 1. Only the failed link fails over. All devices communicating over interface 0 must now also communicate over interface 1. (The data flows over RTCN Switch Group 1 requires all DDP, CCP, and SDC interfaces on Group 1 be active in parallel with those on Group 0.) If SDC data ingestion is required on both switch groups at all times, then a fail over to the secondary SDC MUX is required.

3.2.7.3 SDC NIC Failure, All Fail Over

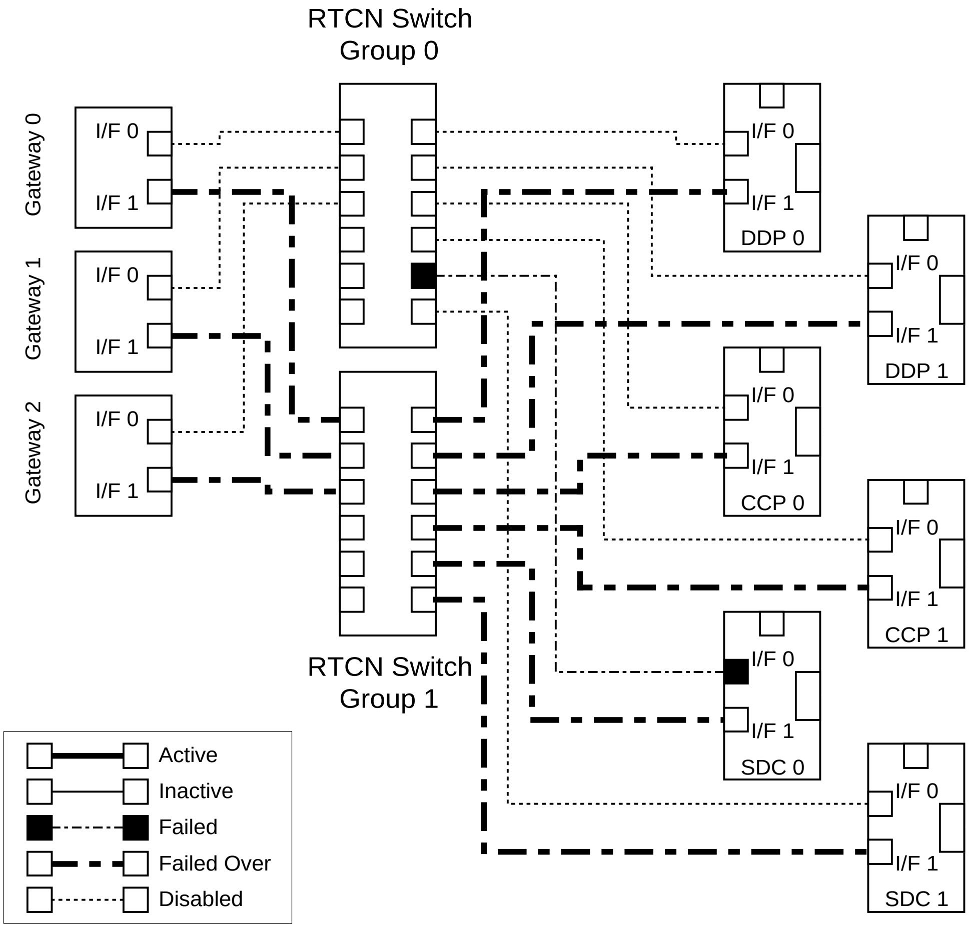

Figure 3-10, SDC NIC Failure, All Devices Fail Over

Figure 3-10 illustrates the case where SDC 0 interface 0 to the RTCN fails. The SDC begins ingesting data on its interface 1. This scenario assumes that the system software swings all data flows onto the secondary paths and completely idles the primary path.

3.2.8 Switch Failure

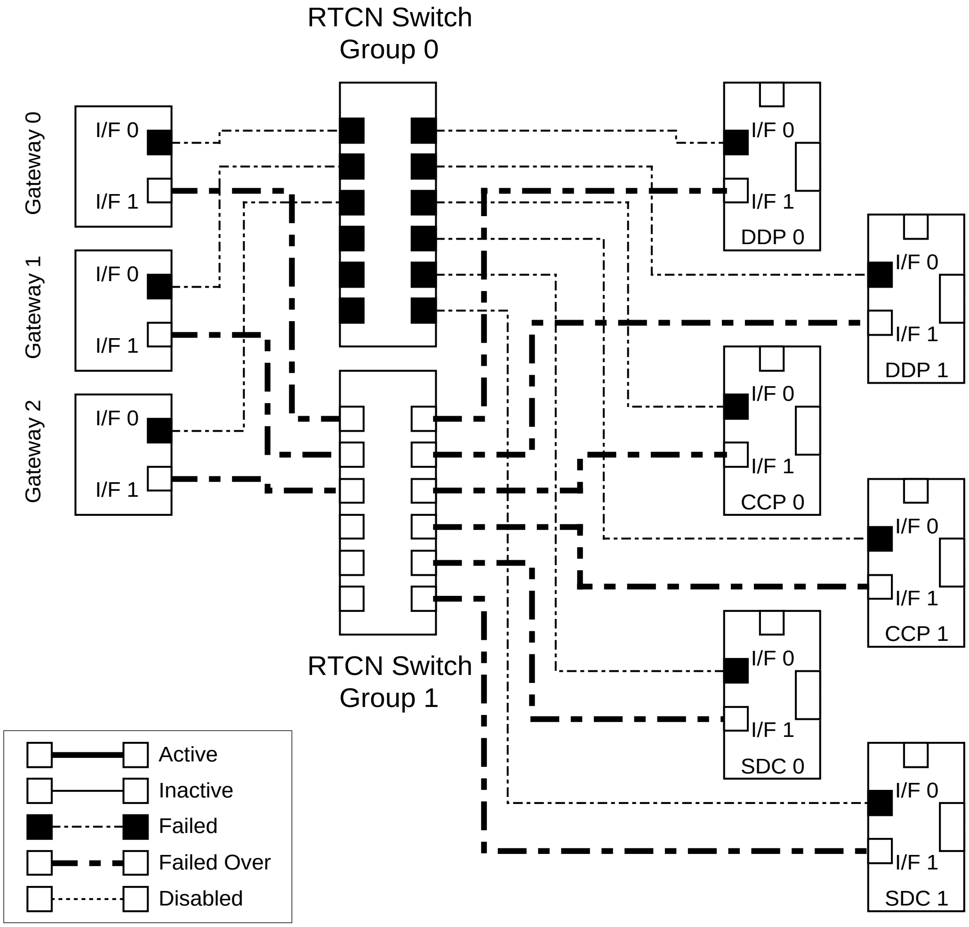

Figure 3-11, RTCN Switch Failure, All Devices Fail Over

Figure 3-11 illustrates the case where a complete switch group fails. All devices begin operations on the secondary paths.

3.3 FAIL OVER MECHANISMS FOR ACTIVE/STANDBY OPERATION

The following sections describe fail over requirements

3.3.1 Impact Analysis

An analysis of the failures described in section 3.2 indicates that there are many different types of failures that result in a loss of connectivity on part of the RTCN. In addition each failure results in the loss of connectivity between different RTPS hosts (Gateways, CCPs, DDPs, and SDC). Since the RTCN simply transports data packets between RTPS hosts and does not differentiate between the packets based on information content, there is no need to develop separate fail over mechanisms for each type of host. Fail over mechanisms can be developed based on how the failure impacts a hosts ability to send or receive messages. By analyzing each of the failures described in section 3.2 it can be determined that each failure on the RTCN results in one of three types of impacts to the ability of the

RTCN to transport messages between hosts. The first type of impact is a failure that interrupts messages between a host sending messages and an RTCN switch Group. The failures that could result in this type of impact are a failure of the network interface card (NIC) on the sending host (referred to as a Sender), a failure of the host's port on the RTCN switch, or a break in the cable connecting the host to the RTCN switch. The second type of impact is a failure between the Switch Group and a host that is receiving messages (referred to as a Receiver). The failures that could result in this type of impact are a failure of a NIC on the receiving host, a failure of the host's port on the RTCN switch, or a break in the cable connecting the receiving host to the RTCN switch. The third type of impact is a failure in the RTCN Switch Group. The failures that could cause this type of interruption are largely dependent on the final architecture of the RTCN switch groups but could include a failure of a single RTCN switch or a failure of a trunk interconnecting two RTCN switches.

3.3.2 Fail Over Mechanism Alternatives

Since the impacts caused by any type of RTCN failures can be categorized as one of the three types listed above, it is only necessary to develop fail over mechanisms to resolve each of these impacts. Therefore, only these types of impacts where analyzed. Some impact types could be resolved using multiple fail over mechanisms, and as a result more than one mechanism was developed in some cases.

3.3.3 Fail Over Mechanism Analysis Approach

In order to resolve any of the three types of failures three actions must be taken. First, the failure must be identified by either the network, the receiver, or the sender. Since the Network Services software uses an Acknowledgment based approach to assure successful delivery of the message, the best way to determine a failure of a connection is by identifying unacknowledged packets. Since the sender becomes aware of an unacknowledged packet, it is logical to use the sender to identify link failures. Once a sender has identified a link failure, an element in the Network must initiate fail over activities. Since the sender identifies the loss of connectivity it is also logical to have the sender initiate the fail over activity. Once the sender initiates the fail over the other senders and receivers must react to the fail over in order to reestablish the required connections. To fully analyze each fail over mechanisms each of the three actions described above were addressed in the analysis. The results of this analysis are described in the following sections.

3.3.4 Sender / Switch Group, Failed Only

Failure between Sender and Switch Group. Sender on failed link fails over to I/F 1.

1. Failure Identification - Sender stops receiving acknowledgments from all registered receivers.
2. Fail Over of other senders - Not applicable in this scenario.
3. Fail Over of receivers -

a) Receiver could be registered for a stream on both I/F. When fail over occurs RM in the receivers would need to be able to receive data over second I/F.

b) As part of fail over, RM in the sender would issue a broadcast message that indicates that fail over has occurred. Receivers would then register for the streams on the new interface.

Issues

1. RM would need the capability to concurrently receive different streams over both interfaces.
2. If only one receiver is registered will not be able to differentiate from Switch Group to Receiver link failure.

3.3.5 Sender / Switch Group, All Interfaces

Failure between Sender and Switch Group. All Senders fail over to I/F 1 and Switch Group 1, no traffic on Switch Group 0.

1. Failure Identification - Sender stops receiving acknowledgments from all registered receivers.
2. Fail Over of other sources -
   a) Sender with failed link sends message to other Senders telling them to fail over to I/F 1 and Switch Group 1.
   b) When a packet is received on I/F 1 the receivers send out messages to Senders instructing the Senders of the streams they are receiving to start using I/F 1 and Switch Group 1. Could be accomplished by modifying the acknowledgments.
3. Fail Over of receivers -
   a) Receiver could be registered for a stream on both I/F. When fail over occurs RM in the receivers would need to be able to receive data over second I/F.
   b) As part of fail over, RM in the sender would issue a broadcast message that indicates that fail over has occurred. Receivers would then register for the required streams on the new interface. This would probably require a table to track which correlates source address and their backup address

Issues

1. If only one receiver is registered will not be able to differentiate from Switch Group to Receiver failure.
2. Senders would need to know which Senders are transmitting streams. Senders would need capability to monitor I/F 1 while transmitting on I/F 0.RM would need to be able to receive fail over instructions.
3. RM would need capability to send out fail over messages from a receiver. There is a possibility that some senders may not be instructed to fail over using this approach.

3.3.6 Receiver / Switch Group, Failed Only

Failure between a receiver and the Switch Group. Fail over streams to receiver with the failed link to Switch Group 1. All other receivers would receive these streams on I/F 0. All streams not destined to receiver with failed link would be unaffected.

1. Failure Identification - All senders stop receiving acknowledgments from a single receiver, but still receive acknowledgments from all other receivers. Sender transmits all streams bound for the receiver with the failed link to I/F 1.
2. Fail over of other senders - All senders currently transmitting to receiver with the failed link will be aware of the failure so notification to these Senders will not be necessary. However the receiver will not be able to add itself to any streams that remain on Switch Group 0.
3. Fail Over of Receivers -
   a) Receiver could be registered for a stream on both I/F. When fail over occurs, RM in the receivers would need to be able to receive data over second I/F.
   b) As part of fail over, RM in the sender would issue a broadcast message over Switch Group 1 that indicates that fail over has occurred. Receivers would then register for the streams bound for the receiver with the failed link on the new interface. Receivers would need the capability to identify which streams were destined to the receiver with the failed link.

Issues

1. If only one receiver is registered, will not be able to differentiate from Sender to Switch Group failure. RM needs to be able to transmit selected streams to the alternate I/F.
2. RM would need the capability to concurrently receive streams over both interfaces.

3.3.7 Receiver / Switch Group, All Interface

Failure between a receiver and the Switch Group. Fail over all streams to I/F 1 and Switch Group 1. No data transmitted over Switch Group 0.

1. Failure Identification - All Senders stop receiving acknowledgments from a single receiver, but still receive acknowledgments from all other receivers.
2. Fail over of other senders -
   a) As a sender switches link it sends message on I/F 0 and Switch Group 0 to other senders telling them to fail over to I/F 1 and Switch Group 1.
   b) When a packet is received on I/F 1 the receivers send out messages to Senders instructing the Senders of the streams they are receiving to start using I/F 1 and Switch Group. Could be accomplished by modifying the acknowledgment.
3. Fail Over of Receivers -

a) Receiver could be registered for a stream on both I/F. When fail over occurs, RM in the receivers would need to be able to receive data over second I/F.

b) As part of fail over, RM in the sender would issue a broadcast message over Switch Group 1 that indicates that fail over has occurred. Receivers would then register for the required streams on the new interface. RM would need to be able to track and compare the sequence number of the packets received on both I/F's.

Issues

1. Senders might need to know which Senders are transmitting streams. Senders would need to be able to receive fail over instructions.
2. RM would need capability to send out fail over messages from a receiver. There is a possibility that some senders may not be instructed to fail over using this approach.

3.3.8 Switch Group

Complete Switch Group Failure. All senders and receivers are forced to I/F 1 and Switch Group 1.

1. Failure Identification - All Senders stop receiving acknowledgments from all receivers. To an individual sender, this failure appears as a local NIC failure. Either each sender independently fails over to switch group 1 or knowledge of the failure must be correlated across multiple platforms.
2. Fail over of other senders - Not applicable. All senders will be aware of the failure.
3. Fail Over of Receivers -
   a) Receiver could be registered for a stream on both I/F. When fail over occurs, RM in the receivers would need to be able to receive data over second I/F.
   b) As part of fail over, RM in the sender would issue a broadcast message over Switch Group 1 that indicates that fail over has occurred. Receivers would then register for the required streams on the new interface. RM would need to be able to track and compare the sequence number of the packets received on both I/F's.

3.4 DUAL STRING GATEWAY PLATFORMS

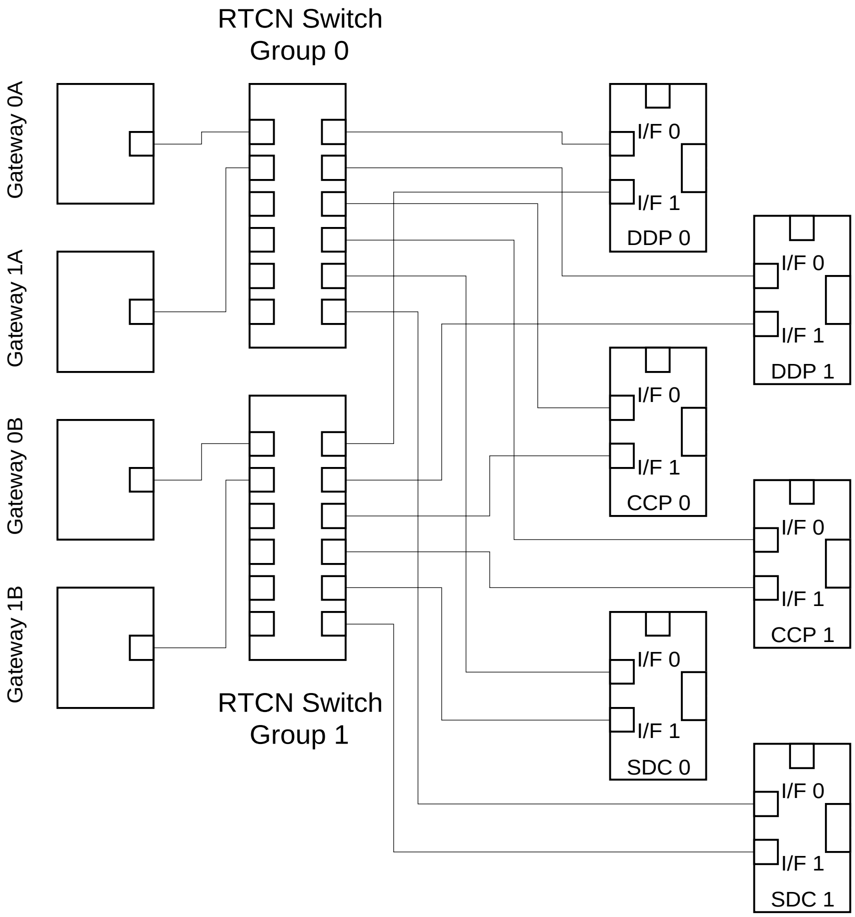

Figure 3-12, Dual String Gateway Platforms

Figure 3-12 illustrates an architecture where the Gateway platforms are equipped with single interface cards and the platforms are provided in redundant pairs where required. The Control Group equipment (DDP, CCP, etc.) maintains two interfaces each for the RTCN network. Fault tolerance and data integrity is not assured if prime and backup Gateway pairs are not provided.

3.4.1 Gateway NIC Failure

A Gateway 0A NIC failure requires fail over of associated processes to Gateway 0B. The redundant interfaces in the DDPs and CCPs allows communication between all DDPs and CCPs and Gateway 0B.

3.4.2 DDP NIC Failure

A DDP 0 Interface 0 NIC failure isolates DDP 0 from the RTCN Switch Group 0 Gateways. Communications with other DDP, CCP, and SDC interfaces are still available through interface 1. This scenario leaves DDP 0 dependent on RTCN Switch Group 1 Gateways while the remainder of the DDPs are operating through RTCN Switch Group 0.

3.4.3 CCP NIC Failure

A CCP 0 Interface 0 NIC failure isolates CCP 0 from the RTCN Switch Group 0 Gateways. Communications with other CCP, DDP, and SDC interfaces are still available through interface 1. This scenario leaves CCP 0 dependent on RTCN Switch Group 1 Gateways while the remainder of the CCPs are operating through RTCN Switch Group 0.

3.4.4 SDC NIC Failure

An SDC 0 Interface 0 NIC failure isolates SDC 0 from the activity on RTCN Switch Group 0. Recording of the traffic on RTCN Switch Group 0 is still available through SDC 1.

3.5 COMPLETE DUAL STRING WITH CROSS STRAP

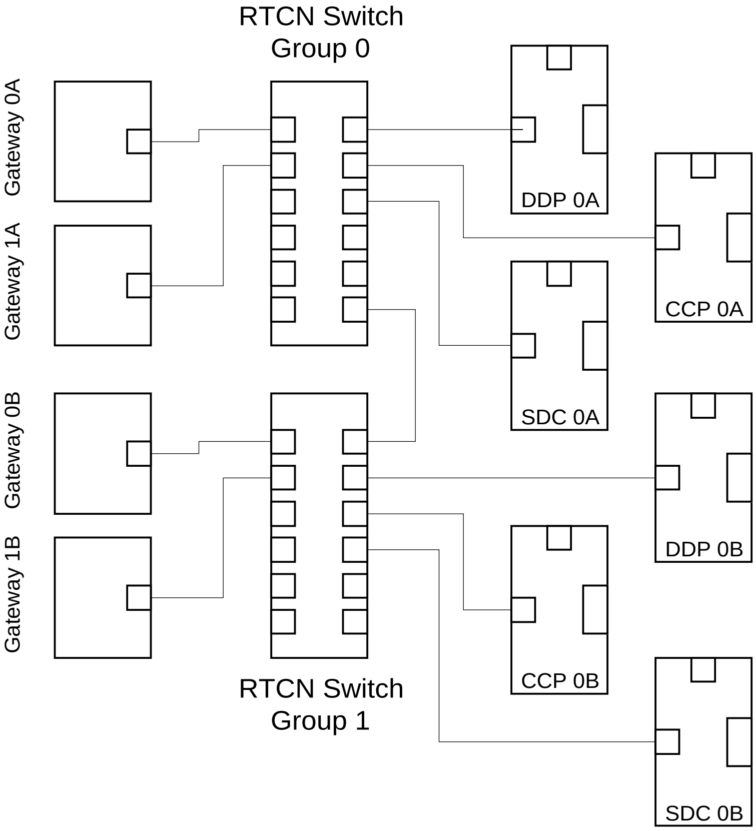

Figure 3-13, Complete Dual String with Cross Strap

Figure 3-13 illustrates an architecture where the Gateway platforms and Control Group equipment (DDP, CCP, etc.) are equipped with single interface cards and the platforms are provided in redundant pairs where required. Fault tolerance and data integrity is not assured if prime and backup pairs are not provided.

3.5.1 Gateway NIC Failure

A Gateway 0A NIC failure requires fail over of associated processes to Gateway 0B. The cross strapping of the two RTCN switch groups allows communication between all DDPs and CCPs and Gateway 0B.

3.5.2 DDP NIC Failure

A DDP 0A NIC failure requires fail over of associated processes to DDP 0B. The cross strapping of the two RTCN switch groups allows communication between all Gateways and CCPs and DDP 0B.

3.5.3 CCP NIC Failure

A CCP 0A NIC failure requires fail over of associated processes to CCP 0B. The cross strapping of the two RTCN switch groups allows communication between all Gateways and DDPs and CCP 0B.

3.5.4 SDC NIC Failure

An SDC 0 NIC failure isolates SDC 0 from all RTCN activity. Recording of RTCN traffic is still available through SDC 1.

4. DCN FAILURE SCENARIOS

4.1 DESCRIPTION

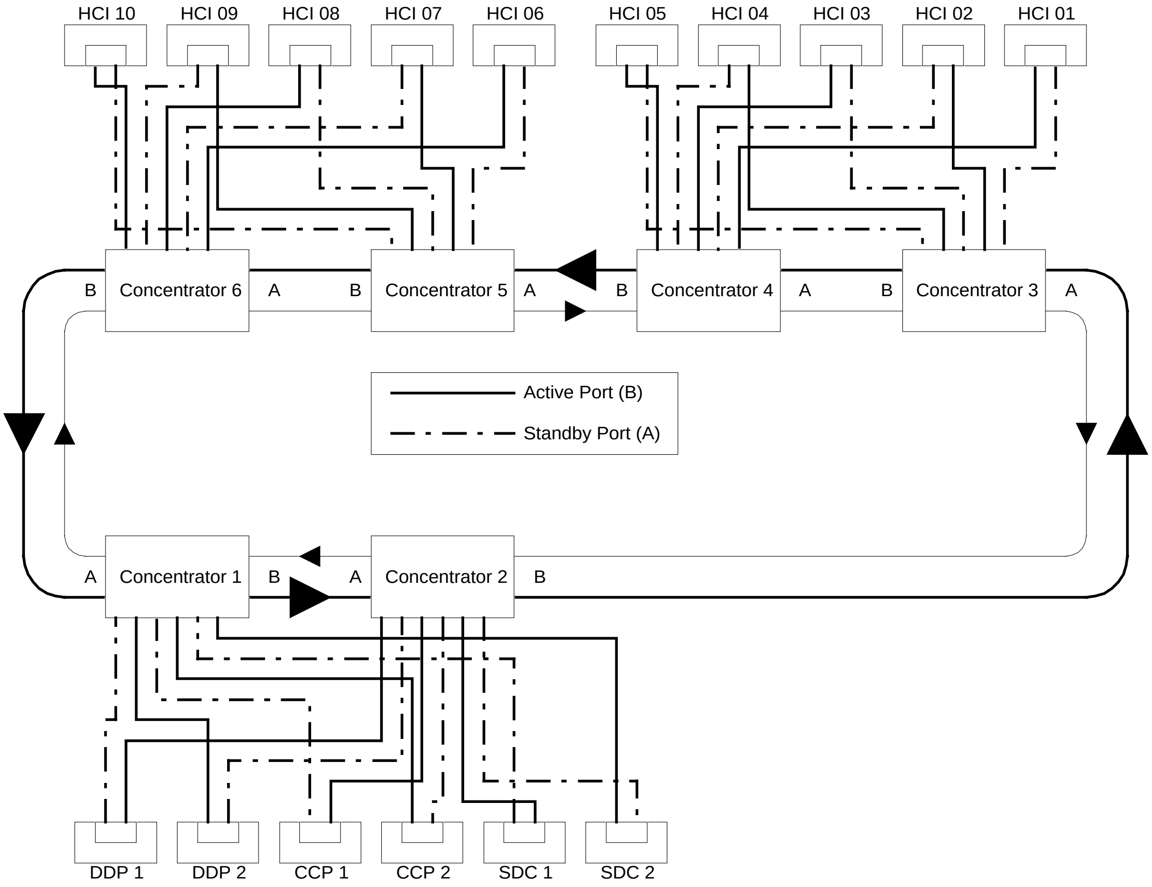

Figure 4-1, FDDI DCN, Nominal Condition

Figure 4-1 illustrates the active data paths in the DCN under nominal conditions.

Communication flows have been identified as:

1. Data transmission:
   a) Data Distribution data from the DDP to the HCI and SDC with associated acknowledgments.
2. Commands:
   a) Command flows from the HCI to the CCP and SDC with associated acknowledgments.
   b) Command Responses from the CCP to the HCI and SDC with associated acknowledgments.

The HCIs are defined as single string devices. Therefore, the DCN does not have RM fail over in contrast to the RTCN.

4.2 NIC FAILURE

Any device has had its interface to the DCN fail. All functionality of the unit with the failed NIC must be moved by system integrity to a redundant piece of hardware

4.3 CONCENTRATOR PORT FAILURE

Any device has had the concentrator port to which it is attached fail. There are two possible scenarios.

1. The concentrator port assign to the A port fails and the unit is never impacted by the failure.
2. The concentrator port assigned to the B port fails and the unit's FDDI NIC automatically begins using the A port .

4.4 CONCENTRATOR FAILURE

If any concentrator fails, the workstations attached by their primary ports all fail over to the paired concentrator, and the workstations attached by their secondary ports are never impacted. This fail over is handled automatically by the FDDI standards.

4.5 SERVICE INTERRUPTION FAILURE

There are scenarios that will cause complete disruption of the FDDI ring for a significant period of time. Describing a generic form for this topic is difficult because experience with the JSC MCC indicates that each of the failures to date have been unique, although of two gross types.

1. Automatic recovery functioned normally, but the ring took significant time to recover.
2. Recovery required manual intervention.

Combined failures have been witnessed on the order of six in five years of continuous operations.

5. CONCLUSIONS

5.1 RTCN SWITCH FAILURES

The RTCN switch groups, although described as a single unit, are actually comprised of multiple switches in a hierarchy. Therefore, failures of individual switches in the group are a possibility. Initial evaluation finds that failures of this type have similar impact to those already discussed, but needs to be revisited.

5.2 COMPLETE DUAL REDUNDANT NETWORKS

If the RTCN is to be as fault tolerant as possible regardless of system integrity considerations, then the baseline architecture is desirable. The placement of dual interface cards in every chassis attached to the RTCN ensures the network viability. Two issues result from this implementation.

1. Every node is attached to both RTCN pieces. There may be a possibility for any single unit connected to both networks to disrupt both simultaneously through hardware failure or software bug.
2. The software and timing required to detect failure and effect fail over using single active data streams is complex and has a good probability of not meeting zero data loss requirements. Therefore, driving and receiving data streams on both interfaces continuously and simultaneously is the desired network option. It is understood that there are be CPU impacts that need to be addressed.

5.3 DUAL STRING NETWORK WITH CROSS STRAP

If the RTCN fault tolerance is factored in with global System Integrity considerations, then a simpler architecture is feasible. Placing single interface cards in each device and creating complete sets of redundant clusters reduces system complexity considerably. Each cluster consists of CCPs, DDPs, and Gateways. Redundant clusters within the same operation have access to each others elements through the cross strap.

5.4 FINAL

The network can be built to be as fault tolerant as possible. It needs to kept in mind that finding a completely COTS solution at the data rates and, more importantly, system synchronous rates involved in the RTCN is not feasible. Developing the required software presents issues with performing fail over in the required interval and maintaining across current and future platforms and operating systems.

Additional questions have to be addressed regarding the method by which the NICs retrieve packets from the network. It is known that some vendor’s NICs perform multicast receive in a promiscuous mode. This means that the CPU possibly has to deal with all multicast traffic on the RTCN regardless of which streams are of local importance.

Appendix A Acronyms and Definitions

<acronym>	*<Definition>*
API	Applications Programming Interface
AT	Acceptance Test - Test to accept hardware and software from a vendor
Certification	Final approval to use a system for a specified set of operations (e.g., hazardous operations in the HMF, launch operations, etc.)
CCP	Command and Control Processor
CI	Configuration Item
CIT	CSCI Integration Test
CLCS	Checkout and Launch Control System
CM	Configuration Management
COTS	Commercial Off The Shelf
CSC	Computer Software Component
CSCI	Computer Software Configuration Item
DAR	Delivery Acceptance Review
DCN	Display and Control Network
DDP	Data Distribution Processor
EDL	Engineering Development Laboratory
FDDI	Fiber Distributed Data Interface
GSE	Ground Support Equipment
HCI	Human Computer Interface
HMF	Hypergol Maintenance Facility
HW	Hardware
HWCI	Hardware Configuration Item
IDE	Integrated Development Environment
I/F	Interface
JSC	Johnson Space Center
KSC	Kennedy Space Center
LAN	Local Area Network
LCC	Launch Control Complex
LMSMS	Lockheed Martin Space Mission Systems and Services
LPS	Launch Processing System

MCC	Mission Control Center
MUX	Multiplexer
NASA	National Aeronautics and Space Administration
NIC	Network Interface Card
MSC	Mission Systems Contract (held by LMSMS)
OS	Operating System
PTR	Post-Test Review
PR	Problem Report
QA	Quality Assurance
QE	Quality Engineering
QT	Qualification Test
RLV	Reusable Launch Vehicle
RM	Reliable Messaging
RTCN	Real Time Critical Network
RTPS	Real Time Processing System
RVM	Requirements Verification Matrix
SDC	Shuttle Data Center
SDE	Satellite Development Environment
SEMP	System Engineering Management Plan
SFOC	Space Flight Operations Contract (held by USA)
SOW	Statement of Work
ST	System Test
SLWT	Super Light Weight Tank
S&MA	Safety and Mission Assurance (includes Reliability, Maintainability, Safety and Quality Assurance)
STS	Space Transportation System
SW	Software
TC	Test Conductor
TCP	Transmission Control Protocol
TPR	Test Progress Review
TR	Test Report
TRR	Test Readiness Review
UAT	User Acceptance Test - Test performed by user community post delivery as part of the system certification process
UDP	User Datagram Protocol
UIT	Unit Integration Test

USA	United Space Alliance
UT	Unit Test
Validation	Testing performed by organization(s) outside of the developing organization to ensure that the delivered system processes data correctly and conforms to the operations concepts

Appendix B Requirements Traceability and Test Methods Matrix

The following table is intended to show which CLCS Functional Requirement is demonstrated in each CLCS <*CSCI/CSC Name*> CSCI Integration Test (CIT) and what test method was used in that test case. This table will be updated and baselined with each CIT starting with the Redstone Delivery.

Functional Requirement	**Traced SLS Requirement**	**CI Test**	**Test Case**	**Test Method**			
				Inspection	**Analysis**	**Demo**	**Test**
N/A							

Appendix C Resource Requirements

This Appendix is not required

Appendix D Standard Test Operating Procedures

This Appendix is not required